KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN 249203)
ak@kazlg.com
Mona Amini (SBN 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff
Haris Mirza

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

HARIS MIRZA, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

23ANDME, INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*;
3. BREACH OF CONTRACT; and
4. NEGLIGENCE

JURY TRIAL DEMANDED

//

//

//

//

//

//

//

Plaintiff HARIS MIRZA ("Plaintiff"), individually and on behalf of the general public and all others similarly situated (the "Class members"), by and through their attorneys, upon personal knowledge as to facts pertaining to themselves and on information and belief as to all other matters, brings this class action against Defendant 23ANDME, INC. ("Defendant" or "23andMe") and alleges as follows:

NATURE OF THE CASE

1. This is a data breach class action arising out of Defendant's failure to implement and maintain reasonable security practices to protect consumers' sensitive personal information. For its business purposes, Defendant stores and transmits personally identifiable information ("PII") from customers including, but not limited to, name, sex, date of birth, DNA and genetic ancestry results, profile photos, geographical information, and other sensitive personal information.

2. On or about October 6, 2023, Defendant publicly announced via its website[1] that customer profile information shared through its DNA Relatives feature[2] was compiled from individual 23andMe.com accounts, without account users' authorization, that contained the personally identifiable information ("PII") and/or protected health information ("PHI") of its customers (the "Data Breach"). Defendant's website notice entitled "Addressing Data Security Concerns" further stated, "[w]e believe that the threat actor may have then, in violation of [Defendant's] Terms of Service, accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users' DNA Relatives profiles."

3. On or about October 11, 2023, Defendant sent Plaintiff and similarly situated Class members additional notifications via email related to the Data Breach,

[1] https://blog.23andme.com/articles/addressing-data-security-concerns (last accessed October 13, 2023)

[2] Through Defendant's DNA Relatives feature available to the company's 14 million users, any account can search for others who may be even a distant genetic match, thus a single account can see the accounts of thousands of other individuals who have information stored or maintained on Defendant's system or network.

which similarly stated, "[w]e recently learned that certain profile information – which a customer creates and chooses to share with their genetic relatives in the DNA Relatives feature – was accessed from individual 23andMe.com accounts. This was done without the account users' authorization."

4. Defendant's Data Breach notifications were misleading and inadequate and did not provide any detail regarding when or for how long the Data Breach occurred. Further, Defendant's Data Breach notices failed to indicate the scope of the Data Breach or the specific information that was accessed, obtained from Defendant's system without authorization and whether any of the PII and/or PHI accessed and/or exfiltrated by the unauthorized person was recovered.

5. Defendant owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard the PII and/or PHI it collected from consumers for business purposes and stored on its systems or networks. This included ensuring information would not be shared with unauthorized parties and that any third-party providers had security procedures in place to maintain the security and integrity of any data to which Defendant gave them access and sufficiently prevented unauthorized access to Defendant's systems.

6. Defendant breached its duty by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect PII and/or PHI from unauthorized access and storing and retaining Plaintiff's and Class members' personal information on inadequately protected systems.

7. The Data Breach happened because of Defendant's inadequate cybersecurity, which caused Plaintiff's and Class members' PII and/or PHI to be accessed, exfiltrated, and disclosed to unauthorized third parties in the Data Breach. This action seeks to address and remedy these failings as Plaintiff brings this action on behalf of himself and all affected individuals.

8. As set forth in the Prayer for Relief, among other things, Plaintiff seeks, for himself and the Class members, injunctive relief, including public injunctive relief, and actual damages.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

10. This Court has personal jurisdiction over Defendant because Defendant maintains a principal place of business within this District in South San Francisco, California and regularly conducts business in the State of California and within this District.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in and/or emanated from within this District.

PARTIES

12. Plaintiff is a resident of Porter Ranch, California, and a citizen of the State of California. Upon information and belief, Plaintiff is a victim of the Data Breach and Plaintiff's information was among the data accessed and/or exfiltrated by an unauthorized third party in the Data Breach,

13. Sometime prior to October 6, 2023, Defendant received or obtained Plaintiff's personal information and/or Plaintiff provided their personal information to Defendant with the expectation that this information would be kept secure and not disclosed to, or permitted to be accessed by, unauthorized parties.

14. On or around October 11, 2023, Defendant sent Plaintiff an email with the subject "Update to our customers." The email informed Plaintiff and other similarly situated Class members of the Data Breach.

15. After learning of the Data Breach, Plaintiff spent significant time and effort taking actions to attempt to mitigate the impact of the Data Breach, including monitoring accounts. This is time Plaintiff otherwise would have spent performing other activities or leisurely events for the enjoyment of life and this loss of time was a direct result of the Data Breach.

16. As a result of the Data Breach, Plaintiff has suffered invasion of privacy and emotional distress as a result of the unauthorized access and disclosure of their PII and/or PHI, which Defendant had a duty to protect from unauthorized disclosure, including anxiety, concern, and uneasiness about unauthorized parties having, viewing, and potentially using their personal information, including DNA information, as well as unease about Defendant having additional data breaches or otherwise disclosing their personal information in the future. In addition to Plaintiff suffering actual injury from lost time and invasion of privacy, Plaintiff also suffers the imminent and continuing injury arising from the heightened risk of fraud and identity theft due to the Data Breach. Upon information and belief, Plaintiff's and the Class members' personal information stolen from Defendant is already leaked and made available for sale and/or purchased by criminals on the dark web.[3]

17. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and maintained, Plaintiff's PII and/or PHI was accessed, exfiltrated, and otherwise disclosed to unauthorized third parties in the Data Breach.

18. Defendant is a corporation formed under the laws of the State of Delaware with a principal place of business located at 349 Oyster Point Blvd, South San Francisco, California.

19. The agents, servants and/or employees of the Defendant and each of them acting on behalf of the Defendant acted within the course and scope of his, her or its

[3] https://www.reuters.com/technology/hackers-advertise-sale-23andme-data-leaked-data-forum-2023-10-06/ (last accessed October 13, 2023)

authority as the agent, servant and/or employee of the Defendant, and personally participated in the conduct alleged herein on behalf of the Defendant with respect to the conduct alleged herein.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

20. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.[4] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

21. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[5]

22. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[6] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

23. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[7]

---

[4] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[5] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[6] *See* Soma, *Corporate Privacy Trend, supra*.

[7] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

24. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

25. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[8] This business has created a new market for the sale and purchase of this valuable data.[9]

26. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

---

[8] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/ 18unboxed.html.

[9] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[10] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1# page_scan_tab_contents.

27. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[11]

28. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

29. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

30. Theft or breach of PII is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[12]

31. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[13] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

32. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and

---

[11]II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).
[12]California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.
[13]*See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[14]

33. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[15] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[16]

34. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[17] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[18] And in 2019, Javelin Strategy & Research compiled consumer

---

[14] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[15] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[16] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[17] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[18] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[19]

35. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

36. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[20]

37. It is within this context that Plaintiff and thousands of other individuals subjected to the Data Breach must now live with the knowledge that their PII and/or PHI was disclosed to unauthorized persons, is likely forever in cyberspace and likely available for sale on the dark web or black market.

Defendant's Business and Collection of Personal Information

38. Defendant was founded in 2006 and began offering direct-to-consumer genetic testing in November 2007 wherein customers, including Plaintiff and the Class members, purchase Defendant's DNA test kits, Defendant's Ancestry Service, Health + Ancestry Service, and/or 23andMe+ Membership, and provide Defendant with their personal information and a saliva sample that is laboratory analyzed, using single nucleotide polymorphism genotyping, to generate reports relating to the customer's ancestry and genetic predispositions to health-related topics, including health reports on genetic health risk, carrier status, wellness, and pharmacogenetics. Defendant also

---

[19]Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[20] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

offers an annual membership that contains everything in the health and ancestry service plus access to ongoing genetic insights.

39. In the course of its business practices, Defendant collects and stores costumers' personal information in its system and networks, including electronically and through its website and mobile applications.

40. Defendant's Privacy Policy,[21] which is incorporated by reference in its Terms of Service,[22] acknowledges that it collects, stores, and transmits a substantial amount of personal information from consumers, including:

- **Individual-level Information:** information about a single individual, such as their genotypes, diseases or other traits or characteristics.
- **De-identified Information:** information that has been stripped of identifying data, such as name and contact information, so that an individual cannot reasonably be identified.
- **Registration Information:** information you provide during account registration or when purchasing the Services, such as a name, user ID, password, date of birth, billing address, shipping address, payment information (e.g., credit card), account authentication information, or contact information (e.g., email, phone number).
- **Genetic Information:** information regarding your genotype (e.g., the As, Ts, Cs, and Gs at particular locations in your DNA). Genetic Information includes the 23andMe genetic data and reports provided to you as part of our Services.
- **Sample Information:** information regarding any sample, such as a saliva sample, that you submit for processing to be analyzed to provide you with Genetic Information, laboratory values or other data provided through our Services.

[21] https://www.23andme.com/legal/privacy/full-version/ (last updated October 4, 2023).
[22] https://www.23andme.com/legal/terms-of-service/

- **Self-Reported Information:** information you provide to 23andMe including your gender, disease conditions, health-related information, traits, ethnicity, family history, or anything else you provide to us within our Service(s).
- **Biometric information:** certain Self-Reported Information you provide to us or our service providers to verify your identity using biological characteristics.
- **User Content:** information, data, text, software, music, audio, photographs, graphics, video, messages, or other materials, other than Genetic Information and Self-Reported Information, generated by users of 23andMe Services and transmitted, whether publicly or privately, to or through 23andMe. For example, User Content includes comments posted on our Blog or messages you send through our Services.
- **Web-Behavior Information:** information on how you use our Services or about the way your devices use our Services is collected through log files, cookies, web beacons, and similar technologies (e.g., device information, device identifiers, IP address, browser type, location, domains, page views).

Defendant's Promises to Safeguard Customer PII

41. Defendant represents and claims that: "We implement physical, technical, and administrative measures aimed at preventing unauthorized access to or disclosure of your Personal Information. Our team regularly reviews and improves our security practices to help ensure the integrity of our systems and your Personal Information."[23]

42. Defendant's Terms of Service agreement incorporates by reference Defendant's Privacy Policy.[24]

[23] https://www.23andme.com/legal/privacy/full-version (last updated October 4, 2023)
[24] https://www.23andme.com/legal/terms-of-service/

The Data Breach

43. On or about October 6, 2023, Defendant publicly announced via its website[25] that customer profile information shared through its DNA Relatives feature was compiled from individual 23andMe.com accounts, without account users' authorization, that contained the personally identifiable information ("PII") and/or protected health information ("PHI") of its customers (the "Data Breach"). Defendant's website notice entitled "Addressing Data Security Concerns" further stated, "[w]e believe that the threat actor may have then, in violation of [Defendant's] Terms of Service, accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users' DNA Relatives profiles."

44. On or about October 11, 2023, Defendant sent Plaintiff and similarly situated Class members additional notifications via email related to the Data Breach, which similarly stated, "[w]e recently learned that certain profile information – which a customer creates and chooses to share with their genetic relatives in the DNA Relatives feature – was accessed from individual 23andMe.com accounts. This was done without the account users' authorization."

45. Defendant proclaimed its data security and safety in its Data Breach notifications which stated, "23andMe is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected;" and "[a]t 23andMe, we take security seriously. We exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected."[26]

[25] https://blog.23andme.com/articles/addressing-data-security-concerns (last accessed October 13, 2023)
[26] *Id.*

46. Defendant's Data Breach notifications were misleading and inadequate and did not provide any detail regarding when or for how long the Data Breach occurred. Further, Defendant's Data Breach notices failed to indicate the scope of the Data Breach or the specific information that was accessed, obtained from Defendant's system without authorization and whether any of the PII and/or PHI accessed and/or exfiltrated by the unauthorized person was recovered.

47. Defendant offered a limited number of recommendations for Plaintiff and the Class members on how to protect against identity theft and fraud. These steps included confirming they had a strong password, using multi-factor authentication (MFA) on their 23andMe account, and reviewing their Privacy and Security Checkup Page. Defendant did not offer Plaintiff and the Class members any identity monitoring services or fraud insurance and failed to address the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and/or fraud.

48. Plaintiff and the Class members' PII stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. be used to commit further identity theft and/or fraud. Plaintiff and the Class members suffer imminent and continuing injury arising from the heightened risk of fraud and identity theft due to the Data Breach, particularly because Plaintiff's and the Class members' personal information stolen from Defendant in the Data Breach is already leaked and made available for sale and/or purchased by criminals on the dark web.

49. Multiple sources, such as NBC News, have reported: "A database that has been shared on dark web forums and viewed by NBC News has a list of 999,999 people who allegedly have used the service. It includes their first and last name, sex, and 23andMe's evaluation of where their ancestors came from."[27]

[27] https://www.nbcnews.com/news/us-news/23andme-user-data-targeting-ashkenazi-jews-leaked-online-rcna119324

Defendant Knew or Should Have Known PII Are High Risk Targets

50. Defendant knew or should have known that PII at issue here, like the personal information of Plaintiff and the Class members, are high risk targets for identity thieves.

51. The Identity Theft Resource Center reported that the business sector had the largest number of breaches in 2018. According to the ITRC this sector suffered 571 data breaches exposing at least 415,233,143 million records in 2018.[28] Further, the ITRC identified "hacking" as the most common form of data breach in 2018, accounting for 39% of data breaches.

52. Prior to the breach there were many reports of high-profile data breaches that should have put a company like Defendant on high alert and forced it to closely examine its own security procedures, as well as those of third parties with which it did business and gave access to its subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a hacker had gained access to 100 million U.S. customer accounts and credit card applications. Similarly, in December 2018, Marriott International announced a data breach that affected up to 500 million individuals. The data breach allowed hackers to access customer names, physical addresses, phone numbers, email addresses, passport numbers, dates of birth, gender, loyalty program account information, and payment card information.[29]

53. As such, Defendant was aware that PII is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiff's and Class members' PII and/or PHI against data breaches and unauthorized disclosures that Defendant should have anticipated and guarded against.

---

[28] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[29] *See* https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach#:~:text=Marriott%20International%20says%20that%20a,up%20to%20500%20million%20people.&text=The%20hotel%20chain%20says%20the,10%2C%202018%20could%20be%20affected

CLASS DEFINITION AND ALLEGATIONS

54. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks to represent and intend to certify a class defined as:

> ***All individuals whose personal information and/or PII was compromised in the Data Breach*** (the "Class").

55. In addition, Plaintiff seeks to represent and intends to certify a sub-class defined as:

> ***All California citizens whose personal information and/or PII was compromised in the Data breach*** (the "California Sub-Class").

56. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

57. Certification of Plaintiff's claims for class wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

58. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, upon information and belief the Class is so numerous that joinder of all members is impractical.

59. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

60. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected from Plaintiff and Class members;

(b) Whether Defendant breached its duty to protect the PII of Plaintiff and Class members; and

(c) Whether Plaintiff and Class members are entitled to damages and other equitable relief.

61. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that they has no interests adverse to or that conflicts with the Class they seek to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

62. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

63. Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code §§ 1798.100, *et seq.*

64. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

65. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[30]

66. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

[30]California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

67. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." 1798.81.5(c).

68. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

69. Plaintiff and Class members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017.

70. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

(a) is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

(b) "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

(c) does business in California; and

(d) has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for

commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

71. The PII taken in the Data Breach is "personal information" as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and Class members' personal information, which upon information and belief includes name, sex, date of birth, DNA and genetic ancestry results, profile photos, geographical information, and other sensitive personal information.

72. Plaintiff's PII was subject to unauthorized access, exfiltration, or disclosure because their PII was wrongfully disclosed and accessed by unauthorized third parties.

73. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII, including to ensure that it had sufficient security protocols in place to protect the PII to which Defendant maintained and/or gave third parties access to. Defendant failed to implement reasonable security procedures to prevent unauthorized access and disclosure of Plaintiff's and Class members' PII as a result of this Data Breach.

74. On or around October 13, 2023, Plaintiff sent Defendant written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Exhibit A. In the event Defendant does not, or is unable to, cure the violation within 30 days, Plaintiff will amend the operative complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

75. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks actual damages, injunctive relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION
Violation of the California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq.*

76. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

77. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning, and in violation of, the UCL.

78. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq*.) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy), Customer Records Act ("CRA") (Cal. Civ. Code §§ 1798.80, et seq., and Civil Code § 1798.81.5. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

79. Defendant also violated the UCL's unlawful prong by breaching contractual obligations created by its Privacy Policies and by knowingly and willfully or, in the alternative, negligently and materially violating Cal. Bus. & Prof. Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of its posted

privacy policy. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of its Terms of Service and/or Privacy Policy.

80. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

81. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of its Privacy Policy and statutory and common law in that a portion of the money Plaintiff and Class members paid, or that Defendant received, for Defendant's products and services went to fulfill the contractual obligations set forth in its Privacy Policy, including maintaining the security of their PII, and Defendant's legal obligations, and Defendant failed to fulfill those obligations.

82. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described claims, nondisclosures and misleading statements were false, misleading, and likely to deceive the consuming public in violation of the UCL.

83. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately

caused the Data Breach and its violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost money or property as a result of Defendant's unfair and deceptive conduct. Such injury includes paying for a certain level of security for their PII but receiving a lower level, paying more for Defendant's products and services than they otherwise would have had they known Defendant was not providing the reasonable security represented in its Privacy Policy and as in conformance with its legal obligations. Had Plaintiff and Class members known about Defendant's substandard data security practices they would not have purchased Defendant's products or services or would have paid less for them. Defendant's security practices have economic value in that reasonable security practices reduce the risk of theft of customer's PII.

84. Plaintiff and Class members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing heightened increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring accounts, and mitigating damages.

85. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself, the Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted

to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

THIRD CAUSE OF ACTION

Breach of Contract

86. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

87. Plaintiff and Class members entered into express or implied contracts with Defendant as set forth in its Terms of Service that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure, as set forth in Defendant's Privacy Policy, which was posted on its website, and expressly incorporated into Defendant's Terms of Service.

88. Plaintiff and Class members performed their obligations under the contracts when they provided their PII to Defendant, or Defendant collected and maintained their PII; however, Plaintiff and the Class members did not receive the full benefit of the bargain from Defendant.

89. Defendant breached its contractual obligation to protect the PII Defendant gathered when the information was exposed to, accessed, and exfiltrated by unauthorized third parties as part of the Data Breach.

90. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

FOURTH CAUSE OF ACTION

Negligence

91. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

92. Defendant owed various duties to Plaintiff and the Class, including pursuant to the CCPA, as alleged in detail above. Defendant owed duties to Plaintiff and the Class with regard to their manner of collection, transmission, sharing, and

maintenance of Plaintiff's and the Class members' personal data, including PII, and were required to maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class members personal information. Defendant further owed Plaintiff and the Class the duty to promptly notify them of the scope and nature of the Data Breach.

93. Defendant breached its respective duties by engaging in the conduct and omissions alleged above and in violation of the CCPA and UCL, as well as its Privacy Policy as alleged above.

94. Defendant is both the actual and legal cause of Plaintiff's and the Class members' damages.

95. Plaintiff believes and thereon alleges that as a proximate result of Defendant's negligence, Plaintiff and the Class have suffered actual damages, invasion and loss of privacy, and emotional distress as described herein and above.

96. Due to the egregious violations alleged herein, Plaintiff asserts that Defendant breached its duties in an oppressive, malicious, despicable, gross, and wantonly negligent manner. Defendant's conscious disregard for Plaintiff's privacy rights entitles Plaintiff and the Class to recover punitive damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all members of the Class respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated a representative of the Class, and (iii) Plaintiff's counsel be appointed as counsel for the Class. Plaintiff, on behalf of himself and members of the Class further requests that upon final trial or hearing, judgment be awarded against Defendant for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) equitable relief, including restitution;

(iii) pre- and post-judgment interest at the highest legal rates applicable;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit; and

(vii) such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all issues so triable.

Dated: October 13, 2023

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: */s/ Abbas Kazerounian*

Abbas Kazerounian, Esq.
Mona Amini, Esq.
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff

EXHIBIT A

KAZEROUNI LAW GROUP, APC

245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

October 13, 2023

VIA CERTIFIED MAIL
23ANDME, INC.
349 OYSTER POINT BLVD
SOUTH SAN FRANCISCO CA 94080

Re: Haris Mirza v. 23andMe, Inc.
Notice of Violations of the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.

To Whom It May Concern:

This office represents Plaintiff Haris Mirza ("Plaintiff") and all other similarly situated consumers in a putative class action against 23andMe, Inc. ("Defendant") arising out of, *inter alia*, Defendant's failure to provide reasonable security for Plaintiff's and the proposed Class members' personal information, which resulted in the unauthorized access, theft, or disclosure of this data (the "Data Breach"). To our knowledge, Defendant has announced the Data Breach via its blog/website beginning on or around October 6, 2023, and via e-mail to Plaintiff and the Class members on or around October 11, 2023.

Plaintiff's claims, including the facts and circumstances surrounding these claims are detailed in Plaintiff's Class Action Complaint, a copy of which is attached and incorporated by reference. Defendant's conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of Plaintiff's claims asserted against Defendant, pursuant to California Civil Code 1798.150(b)(1), in the event a cure is possible, Defendant is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiff with an express written statement within thirty (30) days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiff and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/ Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]